OWWL Library System

2557 State Route 21
Canandaigua, NY 14424

(585) 394-8260
Fax: (585) 394-1935

www.owwl.org

August 19, 2022

TO: Member Library Directors
FROM: Ron Kirsop and CANS Department
SUBJECT: Scanning and Emailing Personally-Identifying Information

Dear Directors,

This memo is to inform you of a recent security breach involving a member library circulation email account. Along with communicating the seriousness of these security breaches, we would also like to share actions that your library should take to mitigate the risk of a breach at your library.

Incident

On August 14, 2022, at 7:39 PM, an unauthorized individual (we'll refer to them as "the hacker") gained access to a circulation email account from a VPN in California. Our logs indicate no password failures, so we suspect a weak password, a phishing scam, or both.

This hacker proceeded to set up several protocols to hide their activity and began sending phishing emails routed through Latvia via this account.

Luckily, a complaint was sent to support@pls-net.org about the phishing messages allowing Bob the opportunity to regain access and lock the account.

Unfortunately, this account was used at the Member Library to help send and receive documents for patrons (via email and/or fax). The account contained 40+ messages with personally identifying information such as SSNs, birth dates, names, email addresses, physical addresses, library card numbers, policy numbers, banking information, driver's license information, etc.

Since personally identifying information was in this hacked account, the library is obligated to comply with the SHIELD Act and notify all impacted individuals of the breach. Failure to do so could result in penalties and fines.

We are working with the System's attorney and the Member Library to ensure we comply with all aspects of the law, including implementing corrective action.

This is not the first data breach that we have faced. However, this instance is a bit more serious because of the content in the account. To give you an idea of the potential financial damages, the last case cost the System $4,661.85 in staff time and legal fees (this instance did not require a data breach mailing to comply with the SHIELD Act).

While hacks and security breaches will never stop, the System is committed to continuing policy evaluation and improving security practices to limit the risk of potential breaches.

We recognize that services involving personally identifying information are important to your patrons. To help limit the risk of potential data breaches, please read the enclosed resource titled, "Scanning and emailing personally identifying information (PII)." This was developed by Kelsy in our CANS department and can be used to amend local procedures that may leave your library at risk in the event of a data breach.

We should all use this situation to better prepare ourselves for future security breaches. Please feel free to reach out with any questions.

Sincerely,

Ronald Kirsop
Executive Director
Pioneer Library System

Scanning and emailing personally identifying information (PII)

We know that many OWWL member libraries offer scanning and emailing services for their patrons. While this is an important service for those who do not have the equipment at home to scan and send their own paperwork, providing this service comes with a risk for both the patron and the library. This is especially true when scanning and emailing paperwork that includes any **personally identifying information (PII)**.

PII is any information that could potentially identify a specific individual, including:

- Full name
- Address
- Date of birth
- Email address
- Phone number
- Social Security Number
- Driver's license number
- Credit/debit card numbers
- Account number and routing number on checks

Having access to even a few pieces of PII enables cybercriminals to commit identity theft.

As stated in Ron's memo, there are legal and financial repercussions if hackers or cybercriminals gain access to patron PII through scanned documents emailed from library accounts.

What can you do to lower the risk of this happening at your library?

1. **Educate your staff.**

   Educate your staff on the dangers of phishing attacks and the legal and financial consequences of a work account being hacked.

   The CANS department is currently developing video and live training options for cybersecurity and phishing awareness. In the meantime, share the following OWWL Docs page with your staff, and encourage them to forward any suspicious emails to support@pls-net.org for analysis.

   https://docs.owwl.org/Members/CommonEmailPhishingScam

2. **Whenever possible, use your printer or copier's Scan-to-Email function.**

   Many of the printers and copiers at member libraries have security protocols in place for scanning and emailing paperwork.

   - Use the printer/copier scan-to-email function to send scanned paperwork directly to the patron's email. They can forward the email as necessary.
     - If the patron does not have an email address, suggest that they sign up for one and assist them in the process.

   - If the patron declines to create an email account, send scanned paperwork to the patron's preferred email destination using the printer/copier scan-to-email function.

   - Printers/copiers have hard drives that may retain images of scanned documents. Check your leasing agreement with your printer or copier vendor. What happens to the hard drive when the lease expires? Is the library responsible for deleting all information?

3. **Don't send scanned emails using a shared email address.**
   If you must send an email on behalf of a patron…

   - Never send scanned paperwork from a shared email address like a circulation or reference email account. If your staff will have a hard time following this rule, assign someone to regularly check and empty the Sent folder on these shared accounts.

   - Instruct staff to use their own email account. As soon as the email is sent, it can be deleted. Left click on the **Sent** folder in Zimbra, right click on the email, and left click **Delete**.
     - Deleted sent emails get moved to the Trash folder. Employees should empty their trash on a regular basis.
     - Emails with sensitive materials should be deleted from the Trash folder immediately.

4. **Use a flash drive.**
   If your printer/copier doesn't have a scan-to-email function, scan the patron's paperwork to a flash drive. Give the flash drive to the patron so that they can log into their own email on a public computer and send the document themselves. **Staff must delete the files from the flash drive between uses so as not to give the next patron access to the previous patron's PII.**

A reminder about password security…

Phishing is not the only way that cybercriminals can gain unauthorized access to online accounts. Accounts with weak or reused passwords are easily hacked.
Encourage your staff to use strong, unique passwords for all of their online accounts, especially ones that may contain confidential library information and patron PII. This includes but is not limited to Evergreen, Google, Intuit/QuickBooks, LibCal (or other event calendars), PayPal, Survey Monkey (or other survey sites), and Zimbra.

Passwords should be easy for the account owner to remember, hard for anyone else to guess, and not reused (repeated) on any other websites/online accounts.

Password managers make it easy to create strong, randomized passwords for all your online accounts—all you need to remember is one password to login to the password manager. If you are interested in learning more about password managers and how they can benefit your library, please contact support@pls-net.org.